

Monday, April 12, 2021

Ann E. Misback
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551
Board Docket No. R-1736, RIN 7100-AG06

James P. Sheesley
Assistant Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429
RIN 3064-AF59

Chief Counsel's Office
Office of the Comptroller of the Currency
400 7th Street SW
Suite 3E-218
Washington, DC 20219
Docket ID OCC-2020-0038, RIN 1557-AF02 (OCC)

Submitted electrically: regs.comments@federalreserve.gov
comments@fdic.gov
www.regulations.gov

Attention: Comments (FDIC)
Comment Processing (OCC)

Re: Notice of Proposed Rulemaking: *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers*.
86 Fed. Reg. 2299 (Jan 12, 2021)
Board Docket No. R-1736, RIN 7100-AG06 (Board)
OCC Docket ID OCC-2020-0038, RIN 1557-AF02 (OCC)
RIN 3064-AF59 (FDIC)

Dear Sir or Madam:

The American Bankers Association (ABA)¹ appreciates the opportunity to respond to the January 2021 notice of proposed rulemaking, *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers* ("Proposal"), jointly issued by the Federal Reserve Board of Governors, the Federal Deposit Insurance Corporation,

¹ The American Bankers Association is the voice of the nation's \$21.9 trillion banking industry, which is composed of small, regional and large banks that together employ more than 2 million people, safeguard \$17 trillion in deposits and extend nearly \$11 trillion in loans. www.aba.com

and the Office of the Comptroller of the Currency (“Agencies”).² On behalf of our members, we welcome the opportunity for further engagement with the Agencies. We share the goal to develop a flexible incident notification framework offering early awareness of disruptions, while also being appropriately scoped to avoid overreporting and unnecessary burden for the banking industry, third party service providers, and the supervisory community.

The comments contained in this letter are the product of weekly meetings over 90 days of the ABA Working Group, a diverse group of ABA members composed of more than 100 people representing 51 banks of varying asset sizes, charter types, and business models.³ This response is a summary of their thoughtful review and robust discussion reflecting on and reacting to the Proposal. In support of the collaborative spirit of the Proposal, the group took a pragmatic approach to consider how early awareness notification could be implemented in a practical, effective manner while being operationally efficient for all financial institutions.

ABA and the ABA Working Group also fully support the suggestions and recommendations made in the letter filed on behalf of ABA, Bank Policy Institute, Institute of International Bankers, and the Securities Industry and Financial Markets Association (“Associations”) in response to the Proposal.⁴ The ABA working group collaborated with the Associations working group assuring both letters actively reflect a whole-of-industry perspective. This letter is submitted as a companion to the Associations’ letter offering further context reflective of the ABA working group’s diversity and operational expertise.

On behalf of ABA’s members and our shared interest in enhancing the Proposal’s efficiency and effectiveness, we respectfully encourage the Agencies to:

- 1) Continue acknowledging the importance of voluntary notice within a larger and expanding notice schema;
- 2) **Recognize the conditional relationship between the sector’s assent to a 36-hour notice timeframe and the need for definitions, expectations, and implementation to be clearly articulated, consistently implemented, and aligned with the Proposal’s light touch-collaborative intent for early awareness notice of operational disruption;**
- 3) Develop flexible notice options that are simple, concise, and utilize existing communication channels; and
- 4) Anticipate adoption over varying timelines as differing needs and compliance resources dictate how institutions will adapt and integrate a new bank service provider notice into existing 3rd party service provider relationships.

² Notice of Proposed Rulemaking and Request for Comment, 86 Fed. Reg. 2299 (Jan. 12, 2021).

³ 49% of the participating institutions were community banks with less than \$10B in assets. 28% of the participating institutions were among the largest 50 banks in the country based on asset size. The group also included two representatives from state banking associations.

⁴ This letter incorporates by reference the comment letter signed by ABA, Bank Policy Institute, Institute of International Bankers, and the Securities Industry and Financial Markets Association and affiliated annexes (*filed* April 12, 2021).

I. Voluntary notice is essential to an efficient notification framework.

Within the evolving notification landscape, there is an essential role for voluntary notice submitted according to a bank's policies, procedures, and business judgement that should continue to be acknowledged and preserved. Voluntary notice incentivizes a bank to report beyond required incidents and offers further insight into sector security and disruption without mandates and compliance burden.

The emerging notification schema would benefit from detailing how the Proposal complements current notification requirements coupled with a policy encouraging the desirable practice of voluntarily notifying on events falling outside of the scope of the Proposal. A common source of concern is the misperception that the Proposal intends to replace existing notice requirements with a short, fixed, prescriptive timeline. There also is concern that the Proposal is overbroad, and would create burdensome overreporting contrary to the spirit of its articulated intent to provide "early awareness" of severe and operationally debilitating occurrences. This concern lies in the belief that the Proposal as written would attach prescriptive mandatory reporting to an array of events, both the actual, materially harmful and extraordinary, as well as the merely possible or mundane. In practice, this would compel banks to overreport nondisruptive events to their primary federal regulator as well as use limited resources to review voluminous overreports from bank service providers.

If the Proposal is reasonably scoped as recommended in the Associations letter,⁵ the acknowledgement of voluntary notice offers a mechanism to report events not causing institution-wide disruption or actual harm due to functioning business continuity plans and sufficient controls and mitigation. These nondisruptive events, however, may be of a type or probability that the bank nonetheless chooses to notify according to internal policy, procedure, or alignment with leading risk management practices. Establishing a clear distinction between mandatory and voluntary notice allows the Proposal to be appropriately tailored. As a result, the proposed notice would focus supervisory and industry resources on actively or severely disruptive incidents, while preserving the supervisory value of reporting nondisruptive events through an alternative voluntary mechanism and timeline.

⁵ Associations letter at 6. (Part II, C) *The Definition of "Notification Incident*. *Infra* at 10 (Part II, D) *The 36-Hour Timeframe for Notification*. *Infra* at 14 (Part II, E).

II. Implementing a 36-hour notice period requires clarity, consistency, and alignment with the Proposal's intent.

The importance of early awareness and the underlying intent of the Proposal's approach is understood and appreciated. However, there remains cautious concern as to how the Proposal will be implemented and enforced.

A. Industry is encouraged by the Proposal's alignment with the standard definition of 'Computer Security Incident.'

In order to avoid the fragmentation observed in other areas of banking law and supervision, it is an industry priority to harmonize cybersecurity regulation and risk management with global standards. Banks across the asset spectrum, from community banks to the largest global financial firms, share this priority and concern. The Agencies' effort, as demonstrated in the Proposal, to rely on the definition of 'computer security incident' as used by the National Institute of Standards and Technology (NIST) is notable and appreciated. Industry is encouraged to see the Agencies looking to global cybersecurity standards, and incorporating those well-known definitions into banking policy and regulations.

In this instance, where the definition of 'computer security incident' was developed for cybersecurity and risk management purposes relative to issues specifically involving the security of consumer information, industry acknowledges that its use in the Proposal is neither tidy, nor precise. However, the use of the term as the first element within a larger notification analysis is adequate, and avoids the construction of a similar, but differing term, that often leads to confusion and later regulatory fragmentation.⁶

B. In keeping with the spirit of the Proposal, the notification requirement should be limited to a set of discrete and rare events grounded in clear definitions and supervisory expectations.

There is strong and diverse support to revise the Proposal to reflect the processes, deliberation, and investigation that an institution of any size would undertake before escalating a notice under the Proposal.⁷ These revisions include replacing the term "believe" with "determine" in the definition of "Notification Incident," and incorporating existing regulatory definitions of events that are reasonably likely to pose actual harm to an institution and can serve as 'landmarks' in an institution's pre-notice analysis.

⁶ "We believe, however, that the term is workable in the proposed rule so long as the definition of "notification incident" is narrowly tailored...to achieve the rule's objectives." Associations letter at 6 "The Associations emphasize, however, that if the NIST definition, which is the subject of ongoing discussion and analysis, is revised in the future, its definition within this rule should also be revised to maintain harmonization." *Infra* at 6, FN 8.

⁷ This letter touches on elements of the Proposal to offer further context and examples. ABA and the ABA Working Group support the full recommendations detailed in the Associations letter (filed April 12, 2021) to refine and revise the definition of "Notification Incident."

1. Determination of “good faith” relies on facts and circumstances.

The moment a bank develops the “good faith” that a rare and discrete incident has occurred is not based on a mere belief. Rather, “good faith” reflects the identification of an incident following a review of the facts and circumstances arising from an event or system anomaly.

In order to shape supervisory expectations, the proposed language should reflect the underlying operational and procedural practices that would form the determination that notice under the Proposal is appropriate. This determination may require the participation of global staff across time zones while gleaning information and recommendations from internal and external stakeholders, experts, and advisors.⁸ At the same time, technical staff will be informing and deliberating with senior leadership. Given the types of disruptive events identified in the Proposal, the board of directors would be engaged for the purpose of notification and concurrence.⁹ As these processes are necessary, often logistically complex, and may not occur promptly, the Proposal’s “good faith” threshold should be revised to rely on the term “determined.”

2. Incorporating existing terms and definitions of discrete, rare, disruptive events will focus the scope of Notice incidents.

To better communicate the types of events of concern, the proposed language may be enhanced by incorporating existing definitions from banking law, regulation, and guidance to serve as signifiers or situational landmarks of an event that is discrete, rare, and reasonably likely to pose actual disruptive harm to an institution. These could include the Prompt Corrective Action (PCA) capital category definitions,¹⁰ or the invocation of Sheltered Harbor protocols to restore critical operational data.¹¹

⁸ Financial Stability Board [FSB], *Effective Practices for Cyber Incident Response and Recovery Final Report*, (October 19, 2020), <https://www.fsb.org/wp-content/uploads/P191020-1.pdf>. Governance, at 4. “Governance frames the way in which [Cyber Incident Response and Recovery] is organised and managed...Governance involves defining the decision-making framework with clear steps and measures of success, and allocates responsibilities and accountabilities to ensure that the right internal and external stakeholders are engaged when a cyber incident occurs. Governance also encapsulates the commitment to support CIRR activities through adequate sponsorship by senior management and to promote positive behaviours dealing with, and following, a cyber incident.” *Effective Practices*, Planning and Preparation, at 7. “Organisations establish lists of internal and external stakeholders to be informed depending on identified scenarios and criteria, *such as on the severity of the incident as well as any required regulatory and statutory notifications* [Emphasis added].”

⁹ Depending on an institution’s governance policies and procedures, informing the board of directors and obtaining their concurrence of a notification incident could be accomplished quickly by email or may be a more complex process requiring a virtual meeting, phone call, or in-person meeting. The process, logistics, and timing will differ for every institution.

¹⁰ Federal Deposit Insurance Act of 1950, Pub. L. No. 81–797, § 64 Stat. 87312 (1950). 38 U.S.C. § 1831o (Prompt Corrective Action). Establishes five Prompt Corrective Action capital categories: well capitalized, adequately capitalized, undercapitalized, significantly undercapitalized, and critically undercapitalized.

¹¹ Sheltered Harbor is a not-for-profit, industry-led standard for protecting and recovering customer account data if a catastrophic event causes critical systems—including backups—to fail. A subsidiary of the Financial Services

Example:

Notice Analysis with PCA Capitalization Thresholds.

Scenario: Ransomware incident. Institution determines in good faith to pay the ransom.

- i. **Payment is of an amount that is reasonably likely to cause the institution to become critically undercapitalized** under the PCA capital category definitions creating an immediate safety and soundness event. The bank should give notice under the Proposal.
- ii. **Payment is not of an amount reasonably likely to cause the institution to become undercapitalized.** There is no actual harm to the institution's capital levels. The institution would not notify under the Proposal. However, the institution may still notify:
 1. Voluntarily to their primary federal or state regulator, in any instance;
 2. As mandated by their state regulator, if required.
 3. According to regulations promulgated under the Gramm-Leach-Bliley Act to inform a primary federal regulator if consumer data may be involved,¹² or
 4. Subject to FinCEN's mandatory or voluntary cyber Suspicious Activity Reports (SARS), as appropriate.¹³

Incorporating well-known banking regulations that define discrete, rare, and severely disruptive elements further clarifies the scope of the Proposal, and brings a sense of familiarity to analysis and implementation.

Information Sharing and Analysis Center (FS-ISAC), its purpose is to promote the stability and resiliency of the financial sector and to preserve public confidence in the financial system in the face of an extended systems outage or destructive cyberattack. The Sheltered Harbor standard combines secure data vaulting of critical customer account information and a resiliency plan to provide customers timely access to their data and funds in a worst-case scenario. www.shelteredharbor.org

¹² The Gramm–Leach–Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, Pub. L. 106–102, 113 Stat. 1338, (November 12, 1999).

¹³ Financial Crimes Enforcement Network (FinCEN), *Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime*, FIN-2016-A005 (Oct 25, 2016).

III. Notice should be flexible, simple, concise, and rely on existing communication channels.

The Proposal's intent to establish flexible and easy notice is welcome.¹⁴ Other notice considerations may include the ability to rescind and the ability to request a record of notice. Institutions may need a mechanism to rescind when initial determinations overestimate the severity or significance of an event or an institution may need to request a record of notice for insurance purposes, especially if notice is delivered by phone or in-person. Notice from a financial institution to their primary federal regulator should be simple, concise, and use existing communication channels.

The incident notice framework should be adequately flexible to accommodate delivery through spontaneous and nontraditional channels. In an extreme disruption scenario, notice may need to rely on whatever communication channel is functioning. This may include delivery by phone or email. It may also include in-person delivery to on-site examiners or staff at a regional office; through an unsecured personal phone or device; or submitted on an existing secure channel, such as FDICConnect. In all instances, a bank should retain the ability to select a method of delivery based on the facts and circumstances of the disruption and the topography of the underlying incident.

IV. Adoption and integration of bank service provider notice will vary with contract terms and compliance resources.

The Proposal's notice obligation for bank service providers is a significant step towards creating a more balanced relationship among financial institutions, the federal banking regulators, and third party service providers. The banking industry is supportive of the creation of a third party notice obligation in concept, and appreciates the direct application of notice requirements, enforcement, and liability for noncompliance on those third parties covered under the Proposal. This is especially important for institutions that may have relatively less ability to impose new and potentially costly contractual obligations on their third party service providers in comparison to larger institutions with often greater leverage in negotiations.

¹⁴ ABA recognizes that each federal banking regulator may further refine the Proposal through agency-specific notice parameters. We welcome these opportunities for further engagement and discussion of the elements and methods of notice.

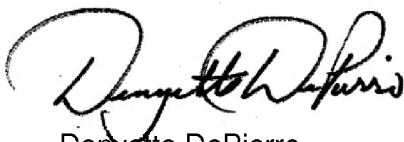
Implementation timelines and supervisory expectations for third party notice should consider time and costs for contract review and revision. Although contracts may include a standard “compliance with all laws” clause, most contracts do not have language mirroring the Proposal requirements:

- When a bank service contract includes standard breach language,¹⁵ it is not uncommon for notice to be required from a service provider within 24 hours. However, standard breach language may not include many of the non-data, operational disruption scenarios contemplated under the Proposal.
- Where contracts require notice for operational disruption, notice to the bank may not be required for several days or weeks after an event.

The ABA Working Group reported that reviewing, revising, and successfully negotiating all service provider contracts through an institution’s usual procurement review process would require a significant amount of time (i.e., on average from 18 months to 2 years). Additional time may be needed if a bank elects to update contractual language at the time of contract expiration, which can be a term of 5-years for many critical services, such as core banking systems.¹⁶ Additional costs include contract review and revision services of in-house procurement and third party risk teams, as well as internal and external experts, such as legal counsel to review existing contract terms, prepare, and negotiate new contract language incorporating the Proposal’s notification requirements.¹⁷ Adoption and implementation will require an extended time after the Proposal is final for contract review and revision.

ABA appreciates the opportunity to respond to the Proposal. Given the ABA Working Group’s robust engagement and ongoing interest in developing an effective and efficient incident notification framework, we welcome the opportunity to collaborate further with the Agencies on the Proposal. Please contact me with questions, or to engage with the ABA Working Group.

Sincerely,



Denyette DePierro

Vice President and Senior Counsel, Cybersecurity and Digital Risk

¹⁵ Not all contracts include standard breach language. The ABA Working Group reported significant variation in the presence and substance of breach language across third party service contracts. An assumption that all contracts contain breach notice is inaccurate.

¹⁶ In some instances, banks are prohibited from revising terms during a contract period, or alternatively, must request modification coupled with a significant renegotiation fee. Hence, many banks, particularly community banks, will elect only to revise contract language according to the renegotiation schedule set by the natural termination of a contract.

¹⁷ The ABA Working Group reported substantial reliance on external experts and consultants to manage negotiations and offer legal review of third-party service contracts. Use of external expertise is reflective of many factors, including the size of the institution as well as the complexity and novelty of the third party service being contracted.